「不正アクセスの高感度検出及び
グローバル警戒機構に関する研究」
報告書

第Ⅴ編　ユーザマニュアル

平成１３年2月

情報処理振興事業協会
セキュリティセンター

目次

1. IDWS

1.1. IDWS システムの概要

1.1.1. 必要条件の分析と設計指針

- IDWS（Intrusion Detection and Warning System：侵入検知及び早期警戒システム）に求められる基本機能は、ネットワークへの不正なアクセスを検出することである。IDWS は指定した広く利用されて高機能化している侵入検知ソフトウェア snort の規則(rules)に合致するパケットを見つけるためのネットワークの監視役(watchdog)のように、機能的であることを意図されている。侵入を検出すると侵入経路の表示と検出結果の解析が行われる。

- SNMP の要素(elements of snmp)を基本とした通信により、IDWS はインターネットに十分配備可能である。

- 一般的なネットワークへの不正アクセス（侵入）への対策として、snort と共に様々な規則を利用できる。

- 警告(alert)メッセージから張られた HTML リンクにより、CERT などのセキュリティ関連組織のサイトへすぐにアクセスでき、豊富な情報を得ることができる。

- このソフトウェアは専門知識の有無に関わらず使用できるように望まれているので、簡単に使用できるべきである。

- ソフトウェアは保守が容易で拡張可能であるべきである。

- ソフトウェアは広範囲で使用可能であるべきである。

- ソフトウェアは容易にダウンロードできるべきである。

1.1.2. 基本設計の概要

IDWS のパッケージはモジュール指向およびオブジェクト指向に基づいて設計されている。後述するパッケージ中のさまざまなモジュールは、機能的な部分(functional blocks)の組み合わせで構成されている。モジュール間の通信は SNMP、Mail、RMI によって行われる。

モジュール指向かつオブジェクト指向の手法を維持することにより、パッケージの保守性、拡張性が保証されている。

1.1.3. 設計の詳細

IDWS はネットワーク内に配備され不正アクセスの発生に伴い警告を発する。そして、パケット sniffer プログラムを利用しネットワークトラヒックとパケットの中身を観測す

ることで、不正アクセスに関する調査を行う。管理システムとなる IDS マネージャは、SNMP メッセージにより不正アクセスに関する情報を通知される。また IDWS は、検出した不正アクセスの状況を可視化するツールでもある。

Sniffer モジュールは、IDWS に組み込みの IDWS 出力プラグインを持つ snort ユーティリティで構成されており、ネットワークトラヒックとパケットの中身を解析し SNMP 通知メッセージの形式で管理システムに向けて警告(Alert)を送信する。マネージャは sniffer モジュールからの警告を受け取ると、INMI（ネットワーク地図情報と連携した捜査診断機能）クライアントモジュールに対して検出した不正アクセスに関して通知する。この通知は Java の Remote Method Invocation の手法を用いて送信される。

IDWS には以下のサブモジュールがある。

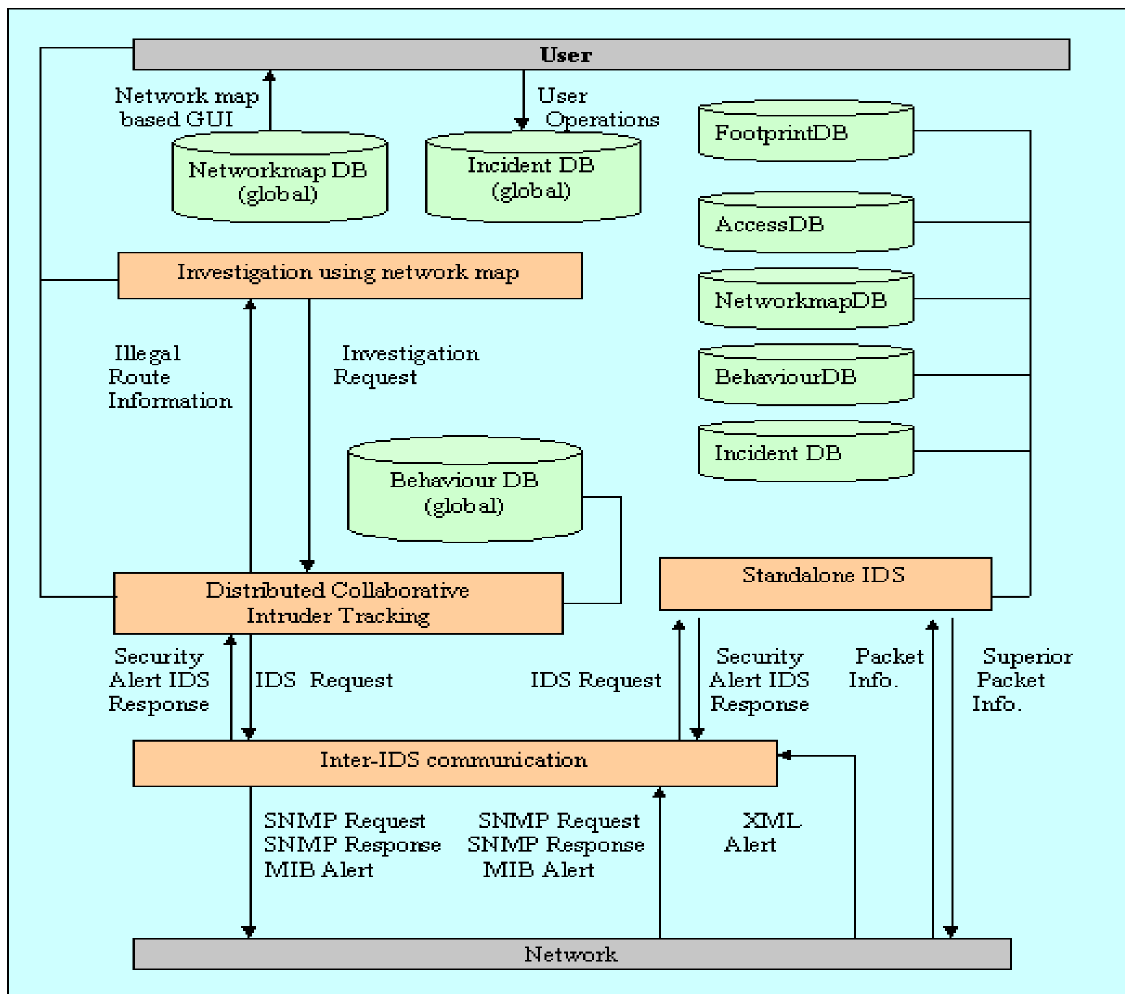
1. セキュリティシステム間通信機能
2. スタンドアローン IDS
3. 分散協調型侵入検出システムアプリケーション
4. ネットワーク地図情報と連携した捜査診断機能

セキュリティシステム間通信機能は、snort に対する output plugin として実装されており、本取扱説明書中では sniffer モジュールの部分として参照される。

スタンドアローン IDS は上記セキュリティシステム間通信機能と拡張された不正アクセス検知機能を備え、本取扱説明書中では sniffer モジュールとして参照される。

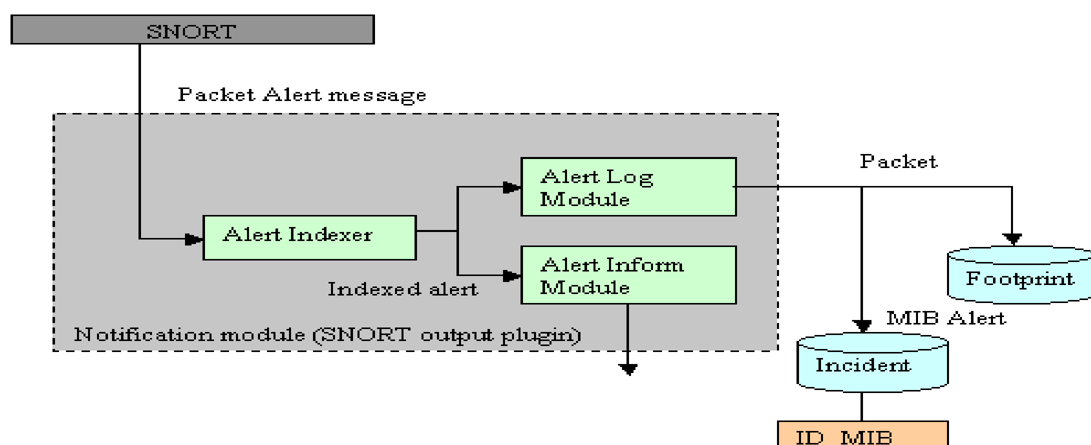
分散協調型侵入検出システムアプリケーションは、上記スタンドアローン IDS とそれらを制御管理する IDS マネージャから成るシステム上で稼動するアプリケーションであり、IDS マネージャの機能として参照される。

ネットワーク地図情報と連携した捜査診断機能は、IDS マネージャのクライアントとして動作し、ユーザへのインタフェースを提供する。



1.1.4. モジュール

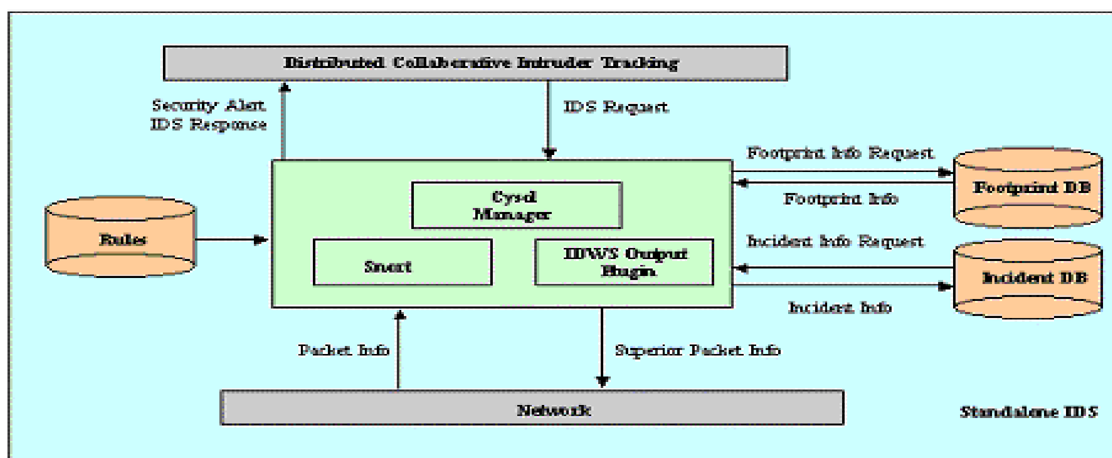
1.1.4.1. セキュリティシステム間通信機能



IDS 間通信モジュールは下記を実行するように設計されている。

- SNMP デーモン（エージェント＋トラップ(trap)/通知(inform)デーモン+API）
  - SNMPv3 のサポート
  - snort のインターフェース
- ID notification MIB のサポート
- XML と SMI 間の変換
  - SMI メッセージから XML 形式への変換
  - XML メッセージから SMI 形式への変換

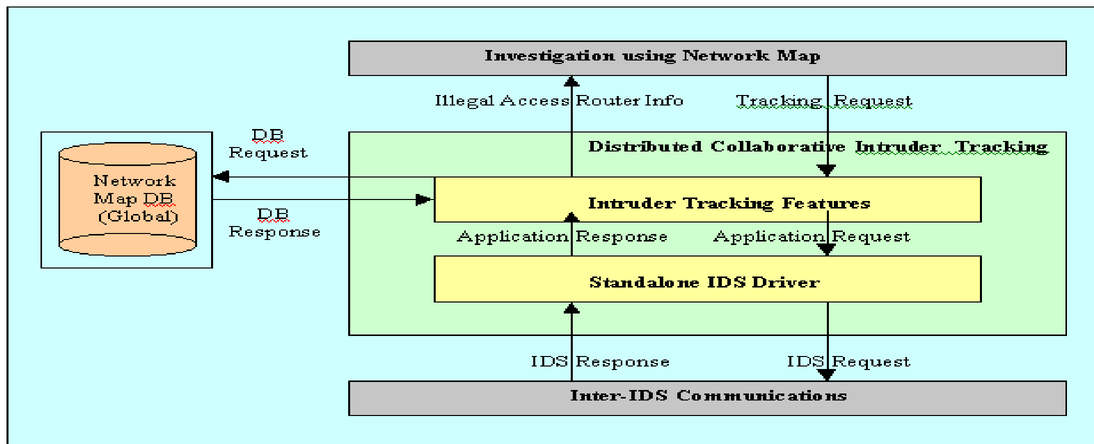
1.1.4.2. スタンドアローン IDS



スタンドアローン IDS モジュールは下記を実行するように設計されている。

- 振る舞い検出の拡張
- Cysol IDS 管理
- Anti-DoS

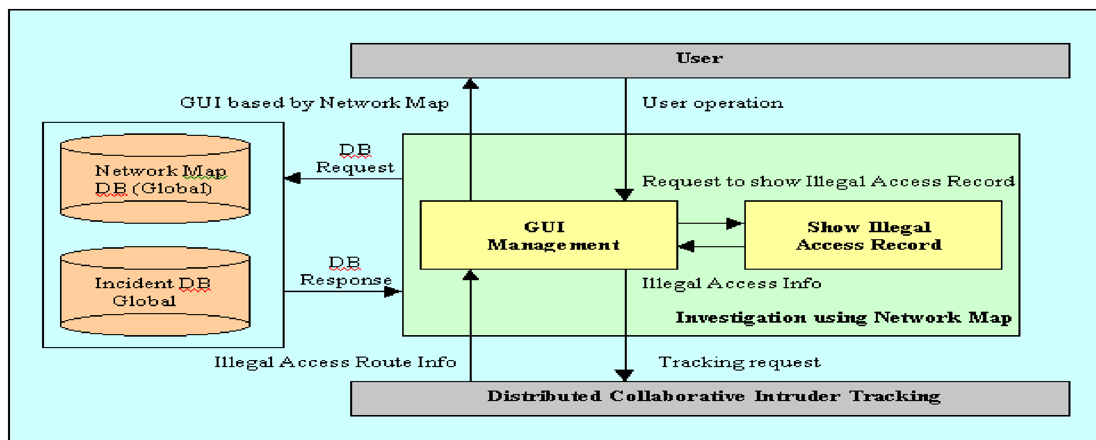
1.1.4.3. 分散協調型侵入検出システムアプリケーション



分散協調型の侵入者追跡モジュールは下記を実行するように設計されている。

- スタンドアローン IDS ドライバ
- 攻撃者追跡
- 広域スキャン検出

1.1.4.4. ネットワーク地図情報と連携した捜査診断機能



ネットワーク地図を用いる調査モジュールは下記を実行するように設計されている。

- GUI によるネットワーク地図の管理
- 不正アクセスの可視化

1.2. IDWS の操作手順

1.2.1. 環境設定

JDK1.3 に付属している *policytool* ユーティリティをアクセス制限のポリシを設定するために使用する。ユーティリティを起動するためには、コマンドプロンプトから以下のように入力する。

% policytool

このアプレットには必要なセキュリティ上の許可を与えることが推奨される。

1.2.2. パッケージの設定

パッケージを起動する前に、パッケージの各モジュールの設定ファイルがユーザ環境に合わせて設定され、保存される。設定の詳細はインストールマニュアルに記載されている。

1.3. IDWS の操作手順

1.3.1. パッケージの起動

パッケージを構成する snort ユーティリティと IDS マネージャおよび INMI は、パッケージを機能的にするために別々に起動する必要がある。

1.3.2. パッケージを起動する前に

RMI レジストリサービス(RMI registry service)が既に起動されている場合は、パッケージの起動時にエラーが発生することがある。そのような時には、以下の様にしてレジストリサービスを終了する必要がある。

% *kill <RMI* ***レジストリサービスのプロセス番号*** >

同様に、snmptrapd が既に起動されており特定のポートを使用しているなら、以下の様にして終了させるべきである。

% *kill <snmptrapd* ***のプロセス番号*** >

1.3.3. Snort ユーティリティの起動

Snort を起動する前に、sniffer/config ディレクトリにある設定ファイル群を/tmp にコピーしなければならない。Snort を起動するには、以下の様に startsnort バッチファイルを使用する。

% cd ~<user>/sniffer

スーパーユーザになってから

% startsnort

以前の snort のログを削除するには、snort 起動後の以下の質問に“ y ”と答えなければならない。

% delete snortlog/alert file(y/n)?

/tmp/AlertID が削除されていた場合警告の通し番号(serial number)は 1 から始まり、そうでなければ以前にパッケージを起動したときの続きから始まる。

ネットワーク内の全パケットは snort により捕捉され、警告のパラメータは SNMP 通知(SNMP INFORM)介して中央の Cysol マネージャに渡される。すべての警告は snort のコンソールに表示される。

SMI メッセージを XML 形式に変換する際の規約がある。XML 形式はメールを介して送信することができる。XML メッセージを受信した側では、メッセージを SMI 形式に変換しなおす。この機能については、インストールのステップで述べたようにに必要なパッケージをインストールしなければならない。

```
Tera Term - zao VT
File Edit Setup Control Window Help
zao_jose% cd public_html/sniffer
zao_jose% su
Password:
# startsnort
rm: remove `snortlog/alert'? y
[?] NOTICE: _PATH_VARRUN is unavailable!
   => Logging Snort PID to log directory (snortlog)

Initializing Network Interface...
   => Decoding Ethernet on interface iprb0
Initializing Preprocessors!
Initializing Plug-ins!
Initializating Output Plugins!

+++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
2 Snort rules read...
2 Option Chains linked into 2 Chain Headers
+++++++++++++++++++++++++++++++++++++++++++++++++++


-*> Snort! <*-
Version 1.6.3
By Martin Roesch (roesch@clark.net, www.snort.org)
Manager      : zao
Engine id    : 800007E501C000001E
incidentDB   : /export/zaohome/jose/public_html/sniffer/data/incident.idb
footprintDB  : /export/zaohome/jose/public_html/sniffer/data/footprint.idb


Alert No : 20001021-1
Alert No : 20001021-2
Alert No : 20001021-3
```

1.3.4. IDS マネージャの起動

IDS マネージャを起動する前に、以下の様に manager/config ディレクトリ以下の設定ファイル群を/tmp にコピーしなければならない。

% cp manager/conf/* /tmp

クライアントである INMI が RMI サーバに正しく登録されるためには、INMI より先に IDS マネージャが起動される必要がある。RMI サーバおよび IDWS マネージャは以下の様に起動する。

% cd ~<ユーザ名>/public_html

% startIDWS

全ての警告の詳細は、設定ファイルである Smp.conf で設定されたパスにある、GlobalIncidentDB.idb ファイルに記録される。

警告処理(alert processing)の詳細もログファイル群に記録される。記録したファイル群は階層構造を形成しており、以下に示す様な場所に保存されている。

idws2/data/logs/<year>/<month>/<day>

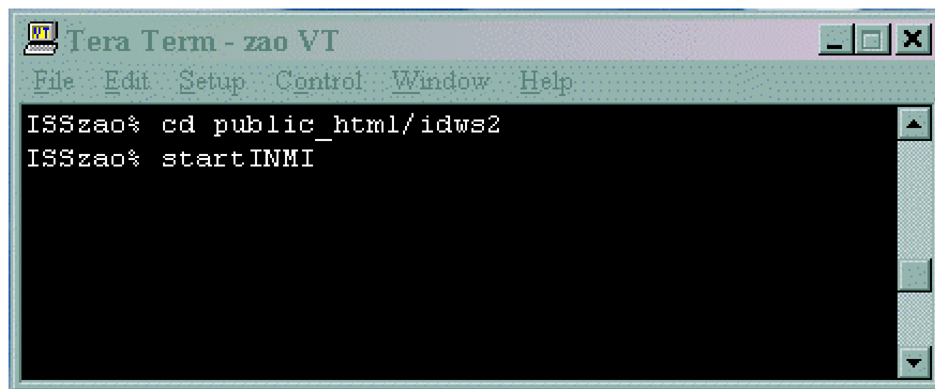
```
Tera Term - zao VT
File Edit Setup Control Window Help
ISSzao% cd public_html/idws2
ISSzao% startIDWS
Loading IRR Server
IRR Remote Server at:zao
-----------------------------------------
IRR Server configured for Map API Queries
-----------------------------------------
-----------------------------------------
Cysol Manager is on Host  : zao/192.0.0.30
SystemLogger Ver. 1.1
Creating the rmiregistry on port 1099...
Successfully created the rmiregistry.
IRRServer is up and running
```

1.3.5. INMI の起動

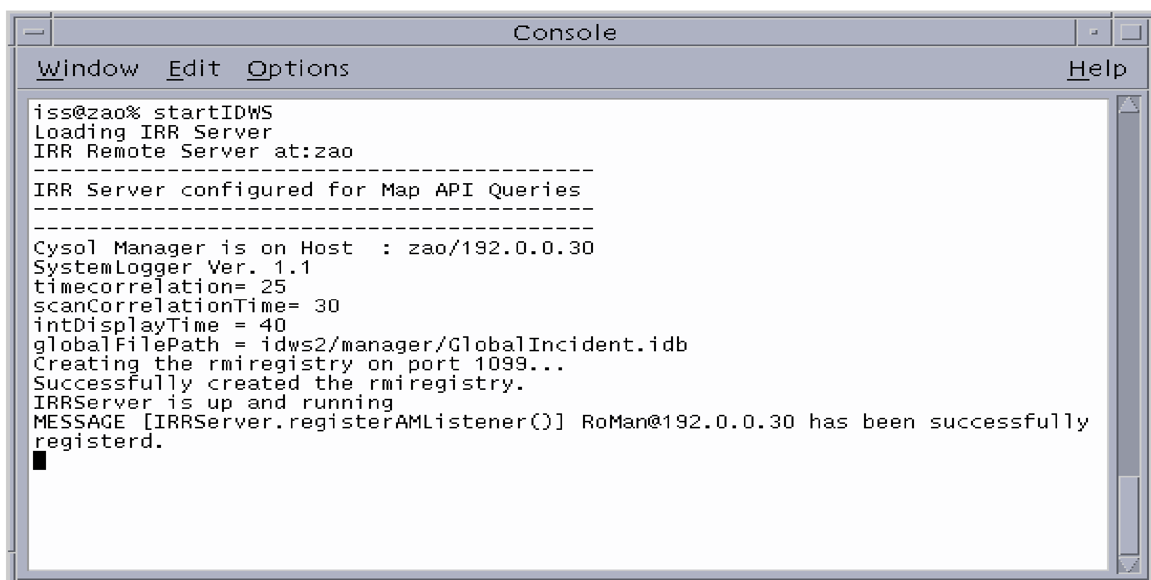
INMI は以下のように起動する。

% cd ~<ユーザ名>/public_html

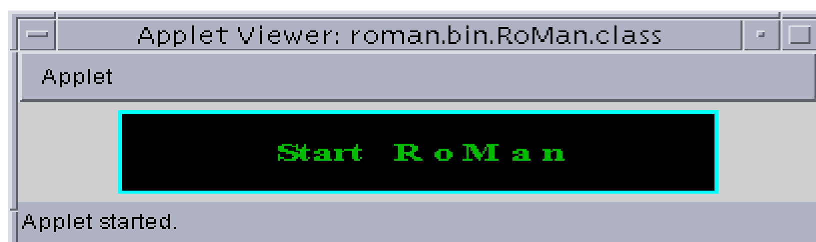
% startINMI



INMIを起動すると、以下のようにメッセージがIDSマネージャのコンソールに表示される。



ネットワーク地図に基づくインタフェースを提供する romanapplet は以下のようにアプレットビューア上で起動される。

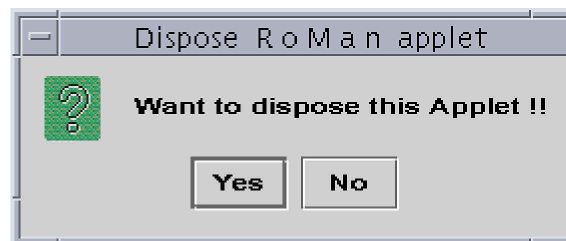


ネットワーク地図を利用した調査を行うには、“Start RoMan”ボタンをクリックする。

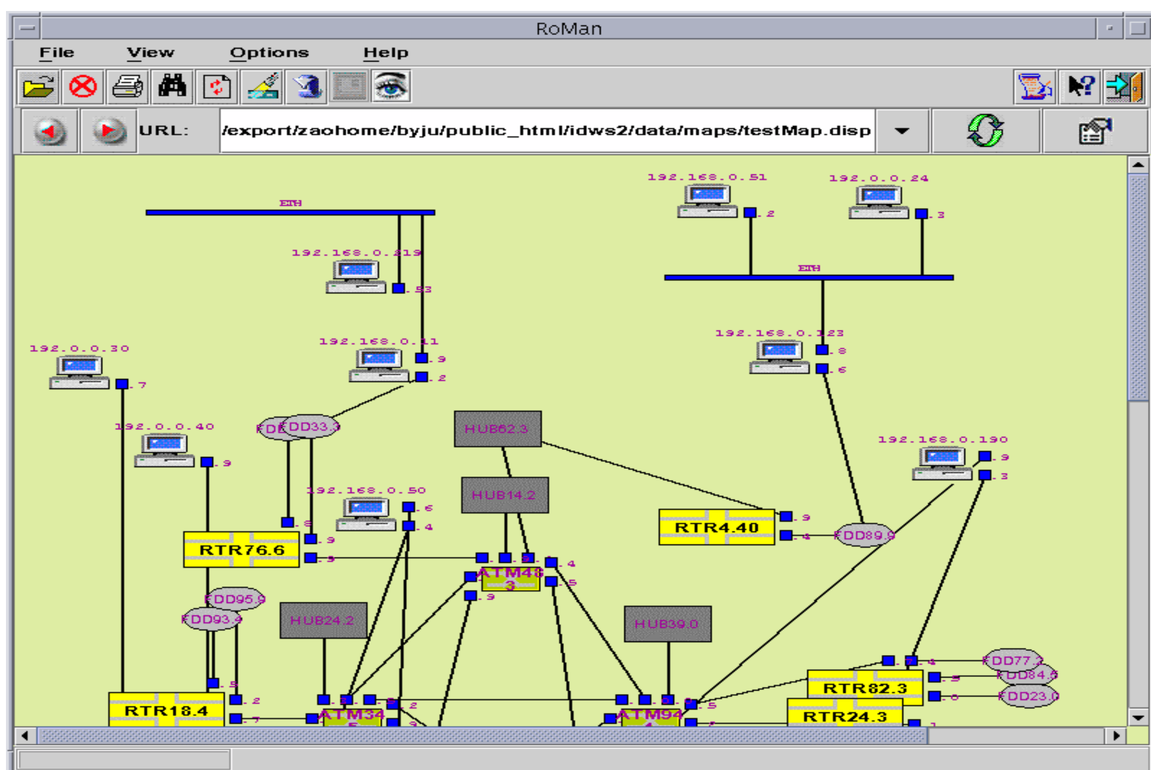
ボタンはアプレットを終了するための“Dispose RoMan”に切り替わる。



“Dispose RoMan”を選択すると、以下のように確認を求めるダイアログボックスが表示される。.

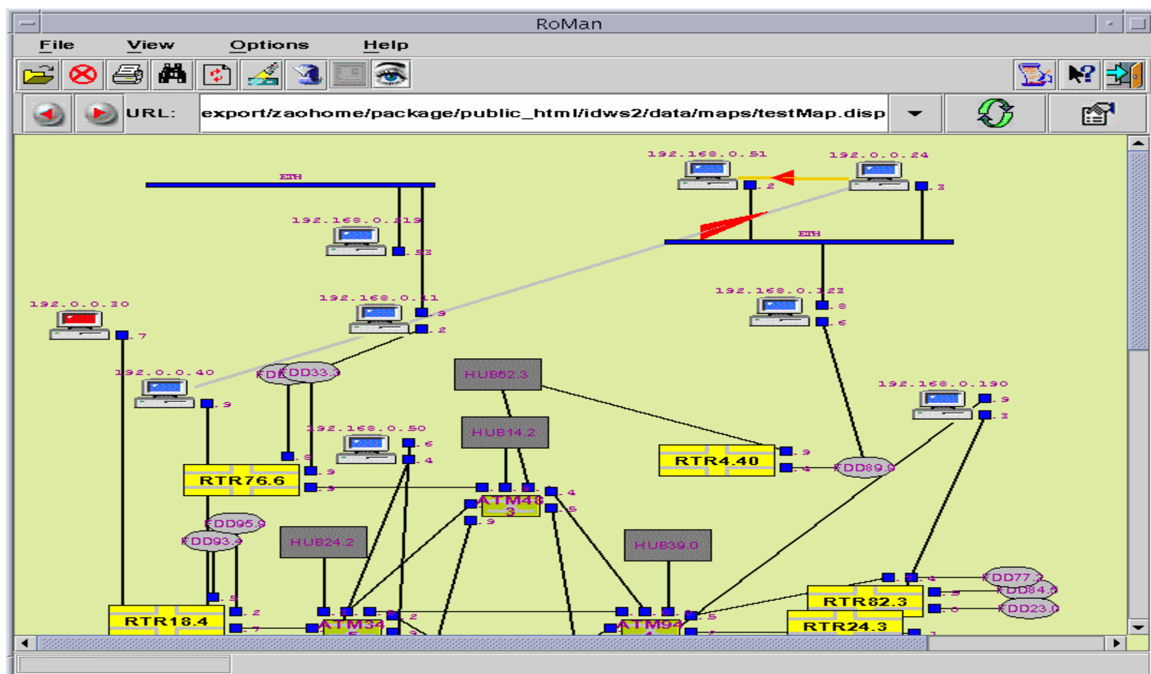


romanapplet が起動されると、以下のようにメインウインドウが表示される。

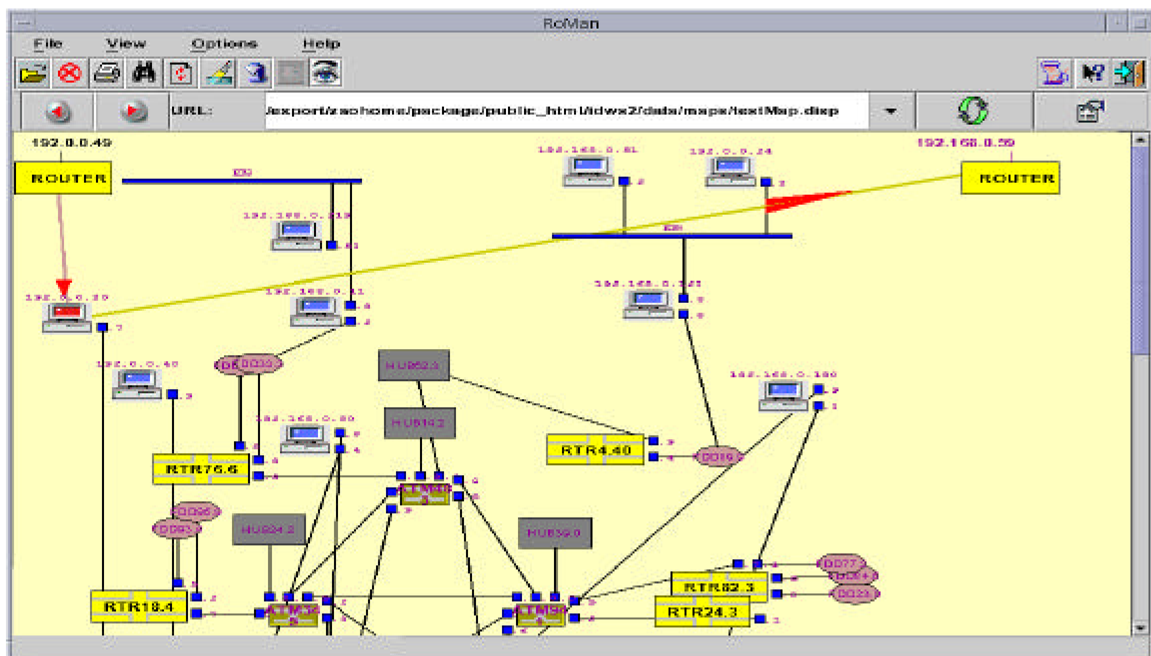


1.3.6. 不正アクセス検出の可視化

ルールファイル(rules file)に従い snort により捕捉された不正アクセスは INMI 上に表示される。不正アクセスが捕捉されると、snort により警告(alert)が発せられ、INMI 上に進入経路が表示される。警告を検出したマネージャが点滅する。

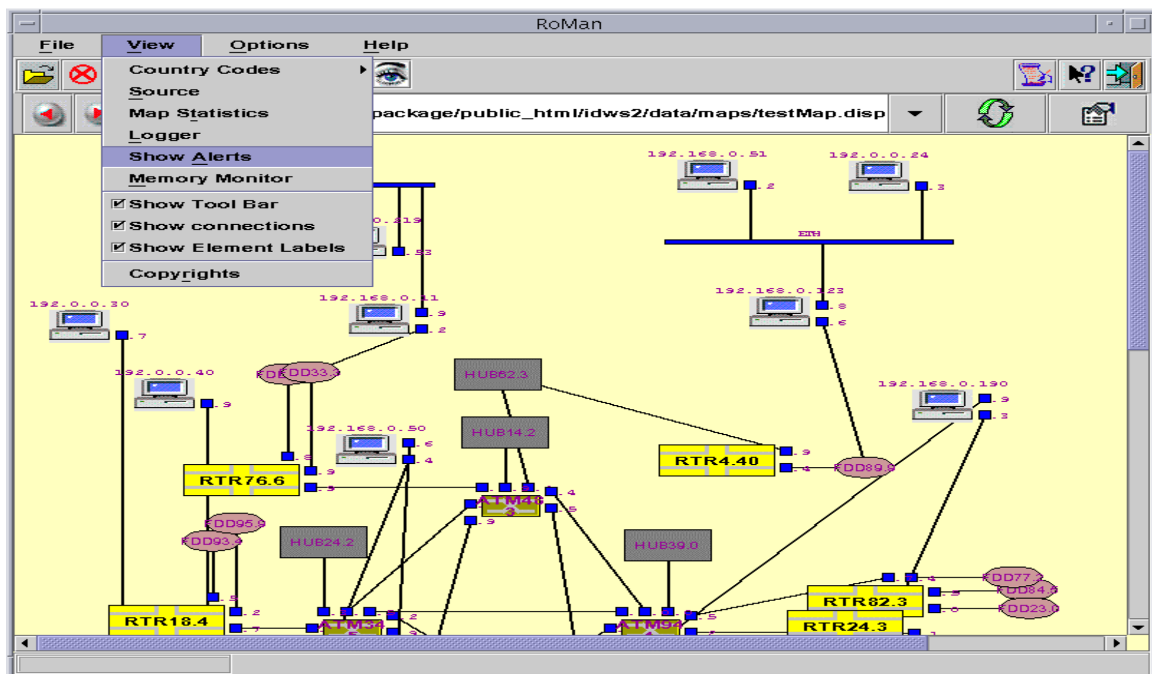


警告の送信元や宛先が地図上に表示されていない場合、下図のように地図の外から始まる進入経路や地図の外へ向かう進入経路が表示される。

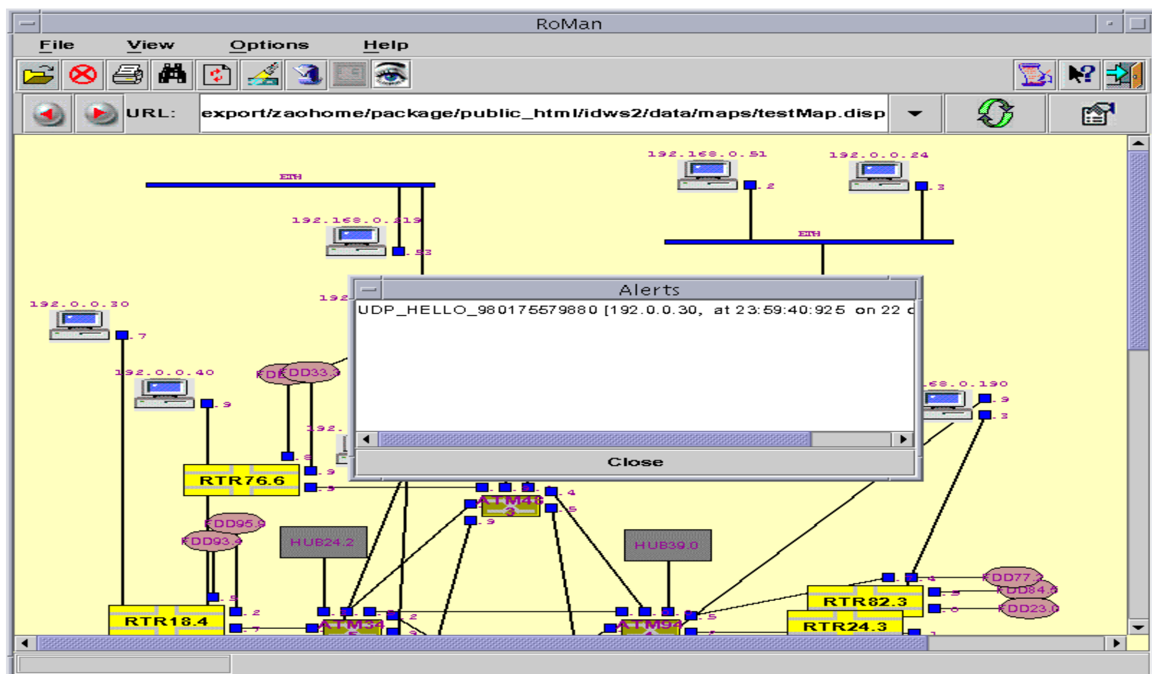


ユーザは INMI 上で以下のような操作を行うことができる。地図上で点滅しているマネージャ上で右クリックすると、”Show Alerts”を含むポップアップメニューが表示される。

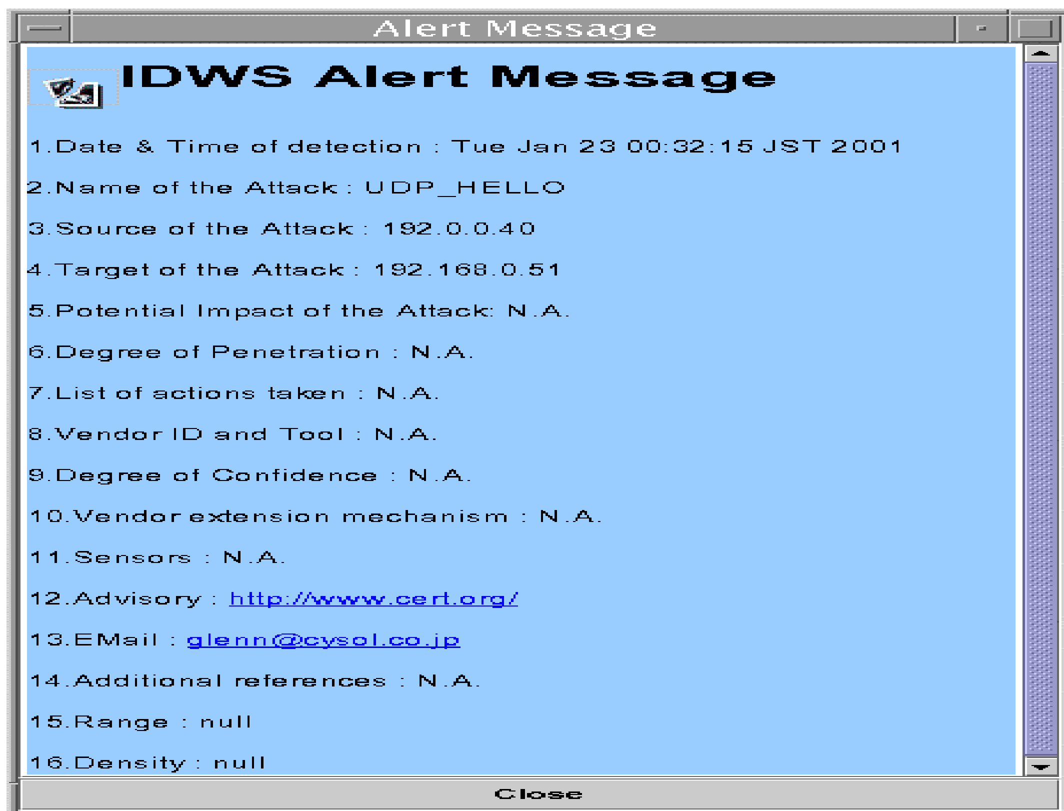
また、”View”メニューから”Show Alerts”を選択しても同じウインドウを表示できる。



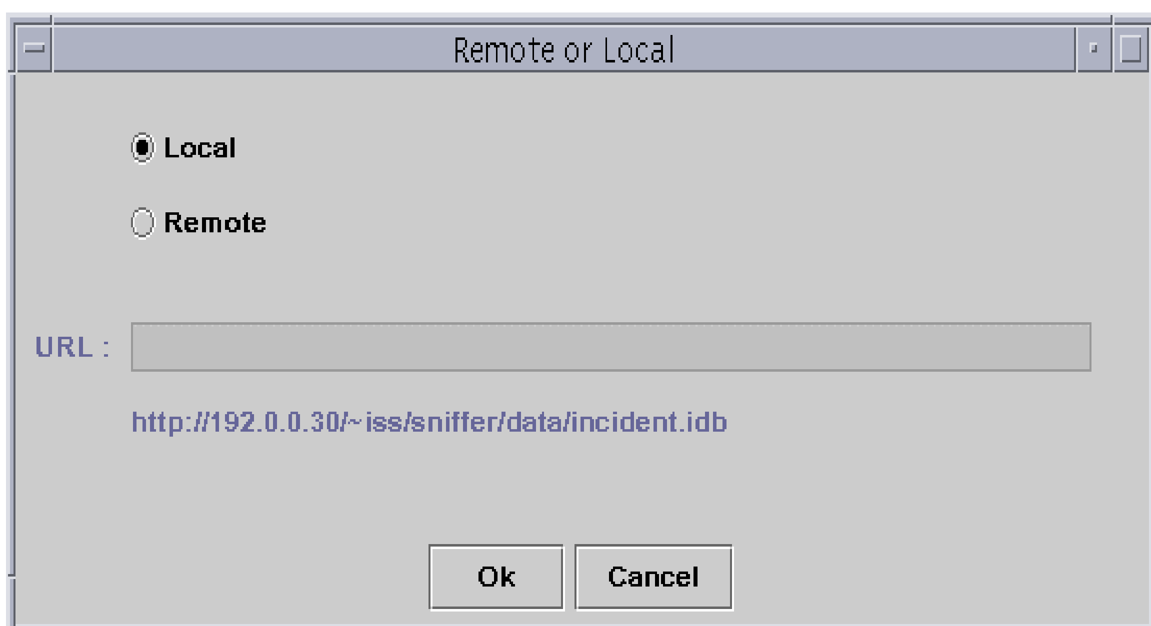
“Show Alerts”をクリックすると、スクロールバーの付いたウインドウ内に警告の一覧が表示される。



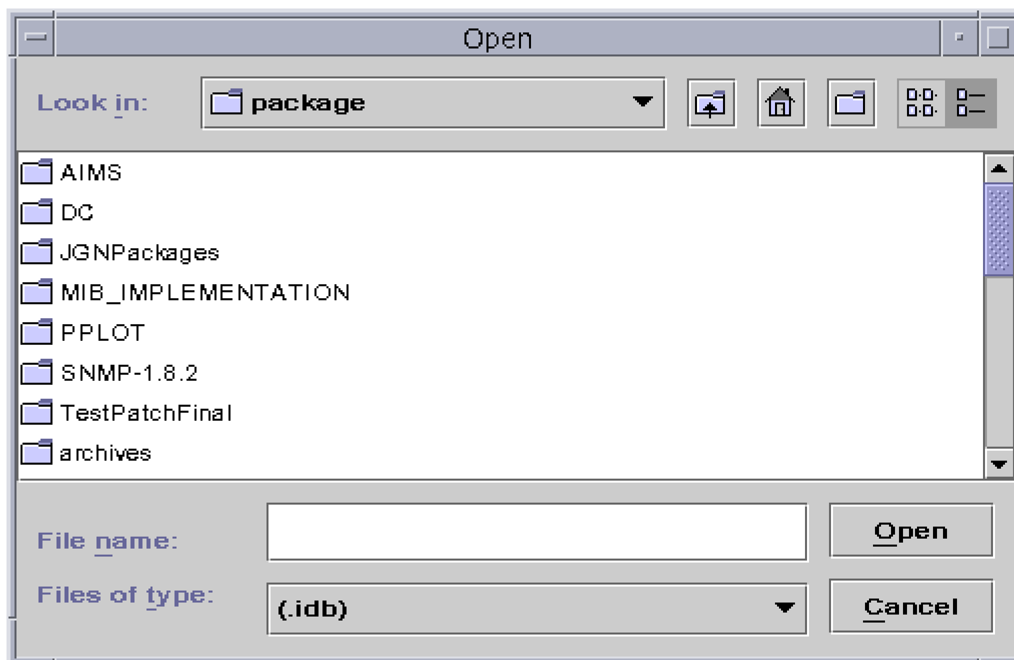
表示したい警告を左クリックすると、その警告が HTML ページとして表示される。この HTML ページは警告の詳細情報を示している。また、警告検知の場合には連絡を受ける関係当局へのハイパーリンクも記載されている。



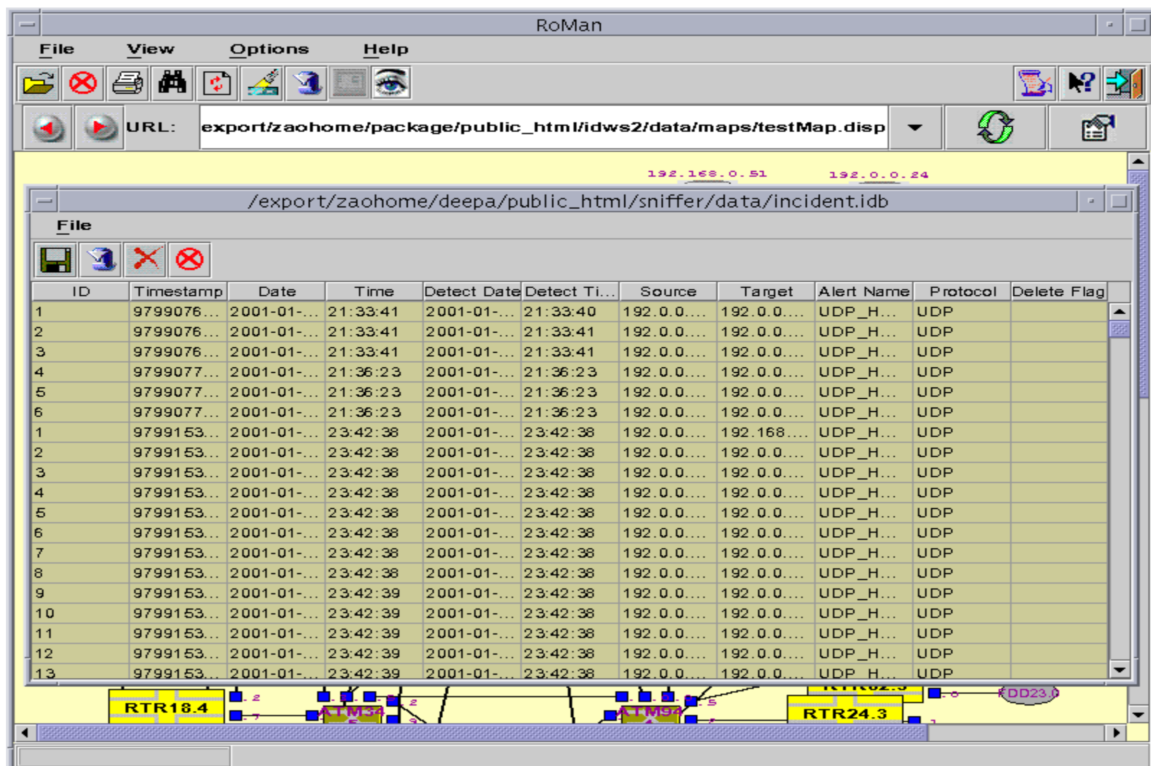
ツールバーから"View"を選択すれば、sniffer ディレクトリ内のデータファイルまたは GlobalIncident.idb ファイルを上図のように編集された形式で見ることができる。



Local もしくは Remote ファイルアクセスオプションを適切に選択すると、以下のようにファイル選択ダイアログボックス(Open File dialog box)が現れる。



適切な警告ファイル(alert file)を選択すると、そのファイルが下図のようにアラートの内容が表形式で表示される。



1.3.7. ツールボタンとメニュー



Open – このボタンを押すと、ファイルダイアログボックスが表示され、開く地図を選択することができる。

Close – このボタンは地図を閉じるために使用する。

Reset – このボタンを押すと、表示されている地図(the selected map)を再描画する。

Reload – このボタンを押すと、地図の再読み込みと解析が行われる。

View Alert Statistics – このボタンを押すと、警告(alert)の送信元と宛先、および警告の種類を適切に抽出することができるようなユーザインタフェースが表示される。その後、選択された送信元と受信先をつなぐ線上にラベルが表示される。

DataBase viewer – このボタンを押すと、ローカルまたはリモートのファイルを選択するためのユーザインターフェースが表示される。選択されたファイルは、表形式で表示される。

Alert Statistics search – このボタンを押すと、警告の送信元と宛先、および警告の種類を選択するためのユーザインターフェースが表示される。選択後にはその警告の詳細が表示される。

1.3.8. XML アラートの表示

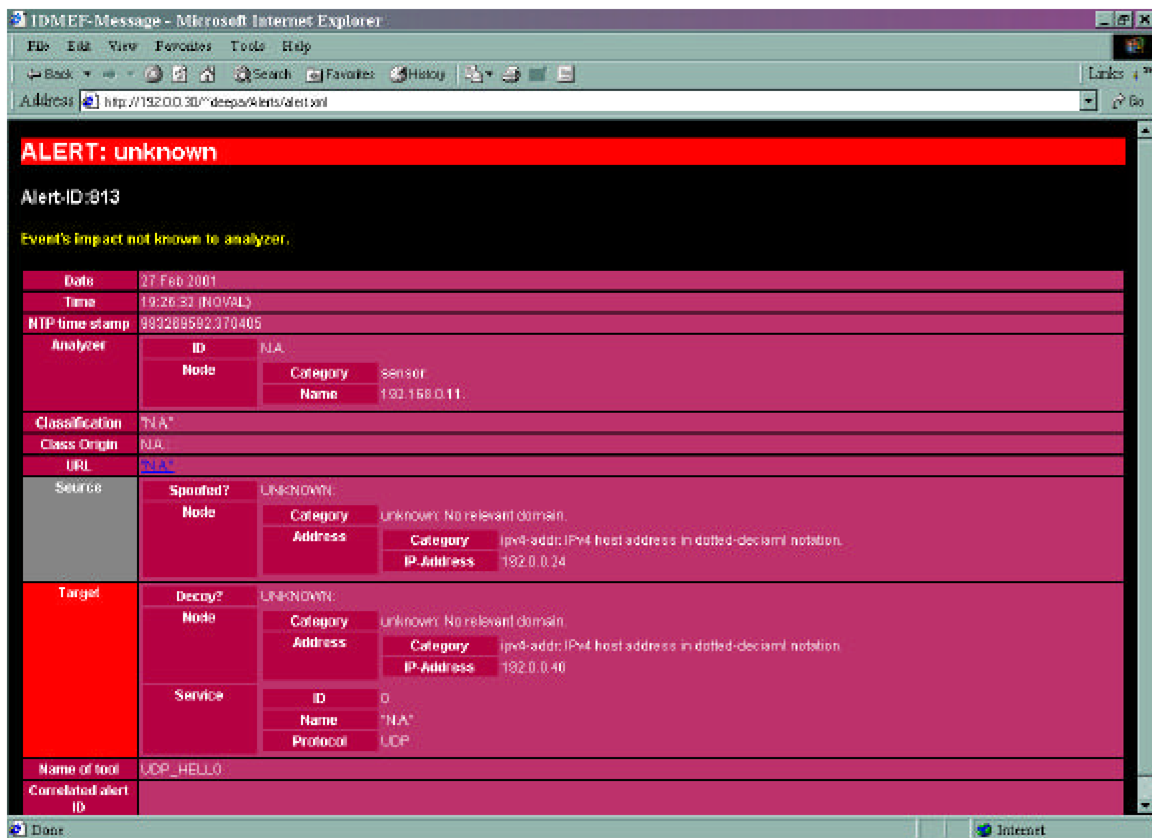
XML ファイルを生成するためには、Smi2Xml プラグインがインストールされている必要がある（プラグインのインストールに関してはインストールマニュアルを参照）。XML ファイルは/var/tmp ディレクトリに生成される。Alert.xsl ファイルがファイルを見るディレクトリにある必要がある(The Alert.xsl file needs to be present in this directory to view the file.)。Alert.xsl ファイルは~user/public_html/Alerts ディレクトリにある。

生成された XML ファイルは E メールによってネットワークを経由して送信される。Xml2Smi プラグインが受信側にインストールされている必要がある（プラグインのインストールに関してはインストールマニュアルを参照）。受信された XML ファイルはインストール時に指定されたディレクトリに置かれる。通常、そのディレクトリは~user/public_html/Alerts ディレクトリである。

XML ファイルを開くには、インターネットエクスプローラ 5.0 以上がインストールされている必要がある。

インターネットエクスプローラを起動し、アドレスに XML ファイルの URL を入力する。例えば、ユーザ idws の URL は以下のようになり、

http://192.0.0.30/~idws/Alerts/192.0.0.30.123333.xml



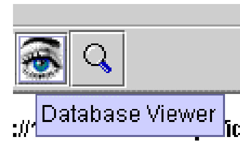
上図の様に、警告の詳細が表示される。代わりに以下のアドレスを入力すると、

http://192.0.0.30/~idws/Alerts/

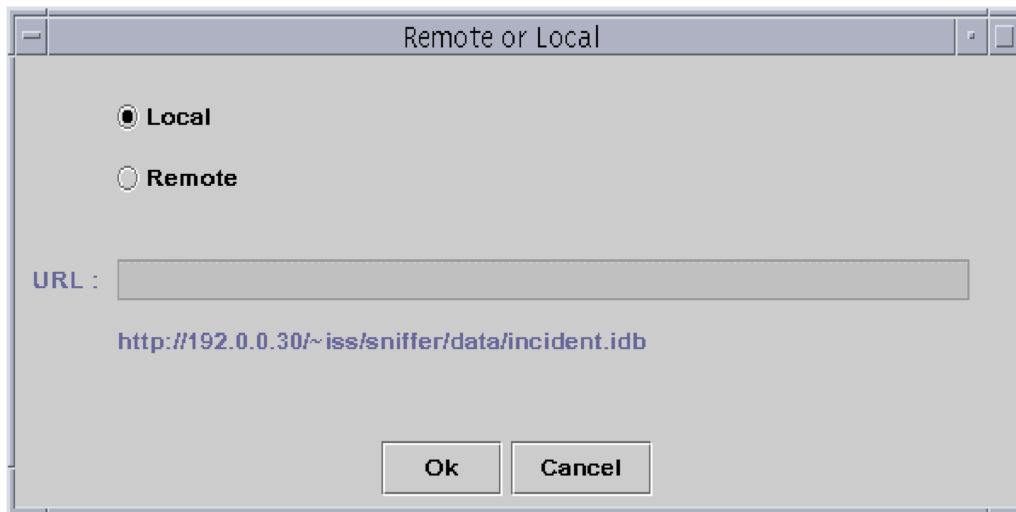
Alerts ディレクトリ内の XML ファイルのリストを得ることができる。

1.3.9. データベースビューア

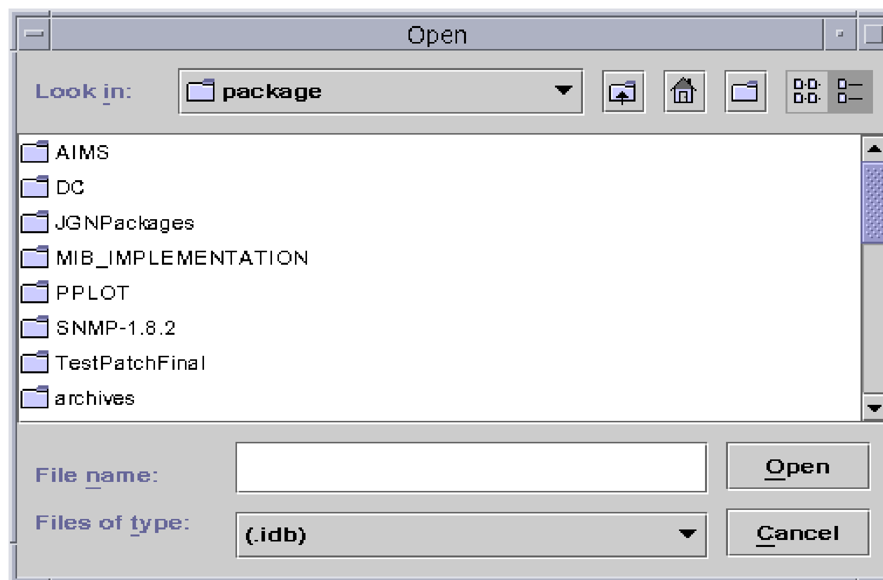
データベースビューアは snort が生成する footprint.idb ファイルおよび incident.idb ファイルを見るために使用する。また、マネージャが生成する GlobalIncident.idb ファイルを見るためにも使用する。データベースビューアを起動するには、ツールバー上の Database viewer ボタンをクリックする。



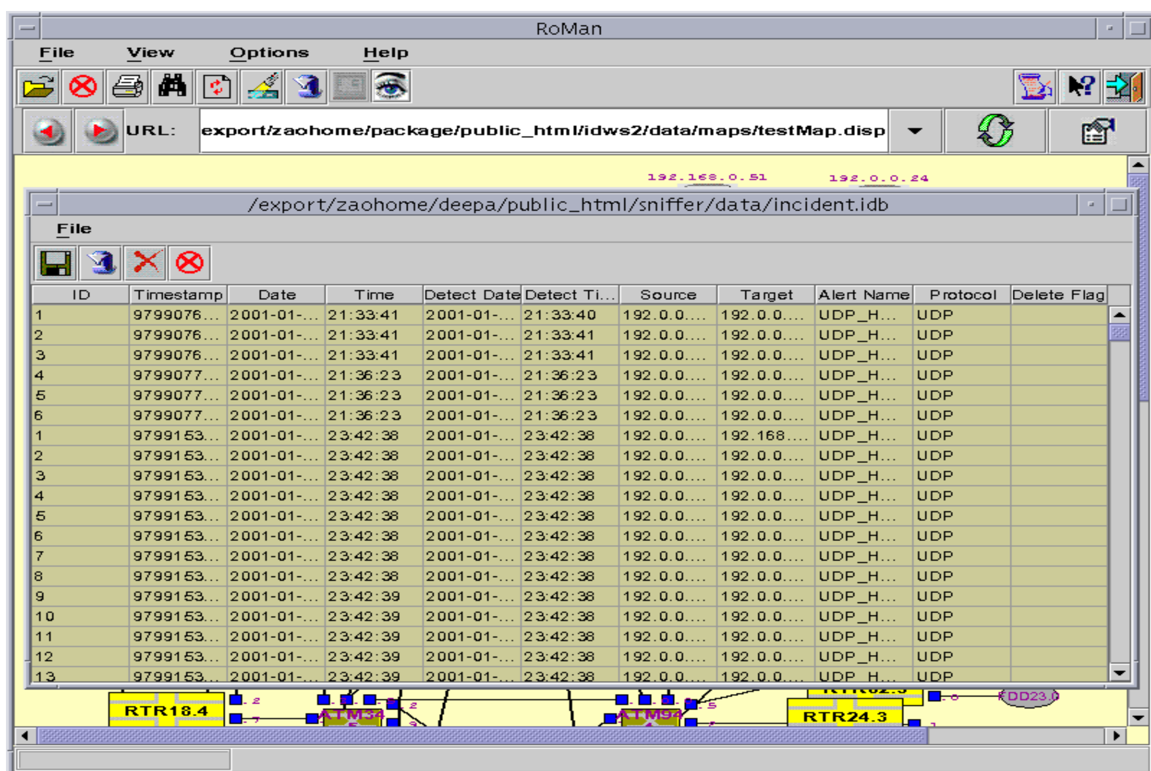
クリックすると以下のようなダイアログボックスが表示され、ローカルかリモートにある開きたいファイルの場所を入力できる。



リモートのファイルを開きたい場合は URL を入力し OK をクリックするとファイルが開かれる。ローカルのファイルを開きたい場合は Local をクリックしてから OK をクリックするとファイルダイアログボックスが表示される。



選択されたファイルの内容が新たなウィンドウで下図のように表示される。



以下の操作が可能である。

- Save

- Reload
- Delete
- Packet Display
- Close

Save

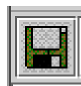
ユーザは削除したいレコードにマークを付けることができる(The user can mark the records for deletion.)。**ファイルからレコードを削除するために、ユーザはファイルを保存できる。このため、ユーザはファイルからいくつかのレコードを削除することができる。**

ファイルを保存するには、

メニューから Save **オプションを選択するか、**



ツールバーの Save tool **ボタンをクリックするか、**



ctrl-S **を押す。**

Reload

開いているファイルを再読み込みするために使用する。ファイルの再読み込みは、

メニューから Reload **オプションを選択するか、**



ツールバーの Reload **ボタンをクリックするか、**



Ctrl-R を押せば行うことができる。

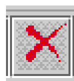
Delete

マークを付けられたレコードを削除するために使用する。ユーザがファイルを保存した時点でそのレコードは削除される。削除を行うには、

メニューから Delete オプションを選択するか、



ツールバーの Delete ボタンをクリックするか、



Ctrl-D を押す。

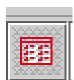
Packet Display

受信した各警告のパケットを表示するために使用する。データベースビューアから警告を選択し、以下のいずれかの方法で packet display を呼び出す。

メニューから Packet Display オプションを選択する。



ツールバーの Packet Display ボタンをクリックする。



Ctrl-P を押す。

選択された警告のパケットの内容は新しいウィンドウで下図のように表示される。

Packet Display

Record Number 7 Type is udp

No	Description	Offset	Length	Value
1	Version	0	1	Version (4: 4)
2	IHL	1	1	IHL (5: 5)
3	Service	2	2	Service (0: 00)
4	Total length	4	4	Total length (33: 0021)
5	Identity	8	4	Identity (242: 00F2)
6	Flags	2	1	Flags (0 0 0 0 : 0)
7	Fragment offset	3	3	Fragment offset (0:000)
8	TTL	6	2	TTL (64: 40)
9	Protocol	8	2	Protocol (udp:11)
10	Header Checksum	0	4	Header Checksum (578...
11	Source address	4	8	Source address (192.1...
12	Destination address	2	8	Destination address (1...
13	Source port	0	4	Source port (8888:22B8)
14	Destination port	4	4	Destination port (6666:...
15	Sequence number	8	8	Sequence number (000...
16	Acknowledgement num...	6	8	Acknowledgement num...
17	Data Offset	4	1	Data Offset ()
18	Reserved	5	1	Reserved ()
19	Code	6	2	Code (0: 00)
20	Window	8	4	Window (0: 00)

Close

Close ボタンをクリックすると、packet display ウィンドウは閉じられる。

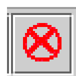
Close

データベースウィンドウを閉じるには、

メニューから Close を選択するか、



ツールバーの close ボタンをクリックするか、



Ctrl-C を押す。

1.3.10. 警告の統計情報

Alert Statistics

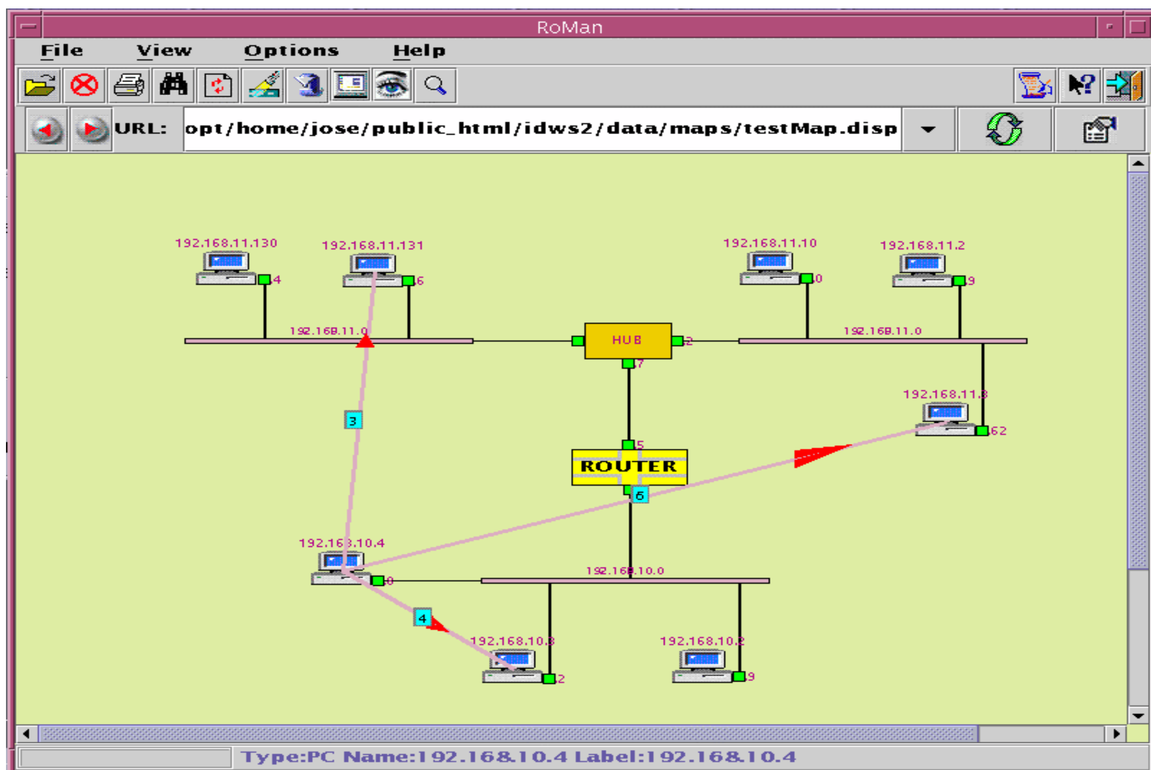
Source *

Destination *

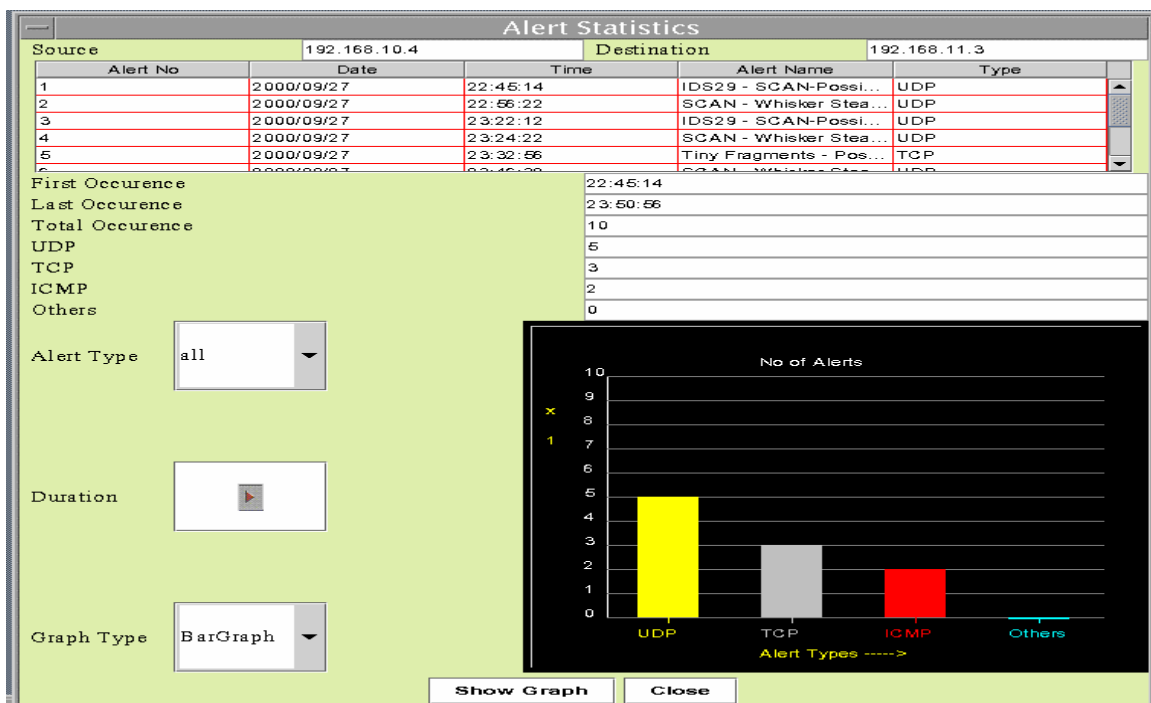
Alert name *

Show Cancel

リストボックス内に一意な(unique)送信元、宛先、警告がある。送信元、宛先、警告を選択後に Show をクリックすると、その警告を見ることができる。選択された送信元と宛先間の警告の総数が以下のように表示される。



警告数(the no of alerts)のラベルをクリックすると、それらの警告が以下のように表示される。



このユーザインターフェースは警告の日時、数、種類、名前に関する情報を与える。また、警告の最初と最後の発生時刻および発生総数の情報も表示されている。

Alert Type コンボボックス(combo box)には以下のオプションがあり、

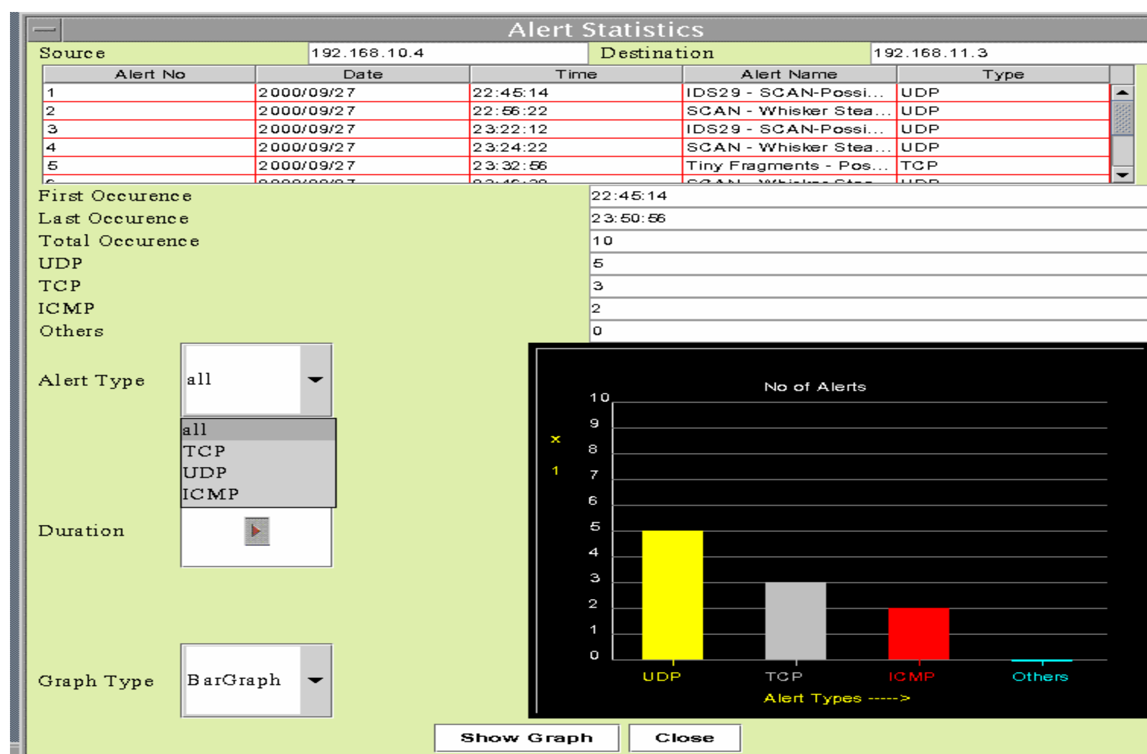
All

UDP

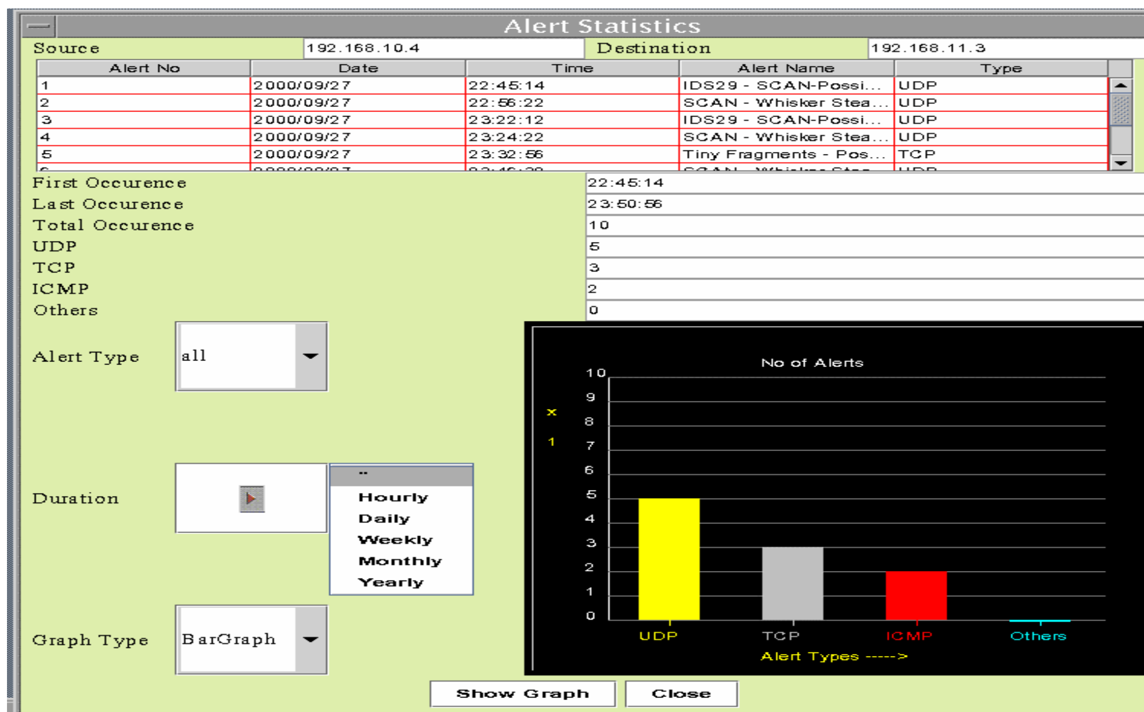
TCP

ICMP

この中のどれを選んでもよい。



Duration ポップアップメニューでは様々な継続時間(duration)を選択できる。



“Hourly”を選んだ場合には以下のようなインターフェースが表示され、この中から選ぶことができる。

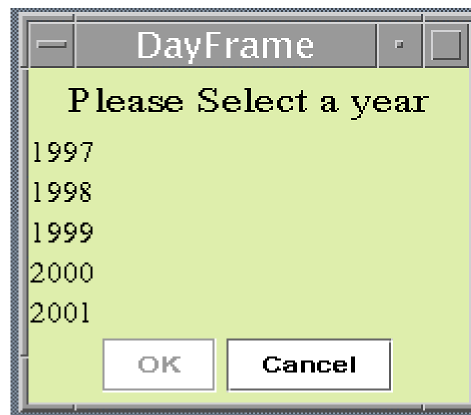
Hours of the Day

Please Select an hour of the day

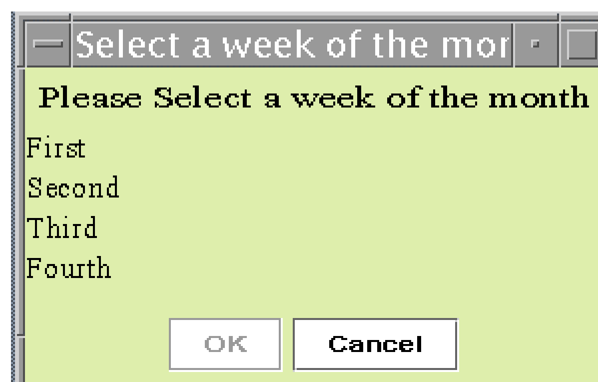
0:00
1:00
2:00
3:00
4:00
5:00
6:00
7:00

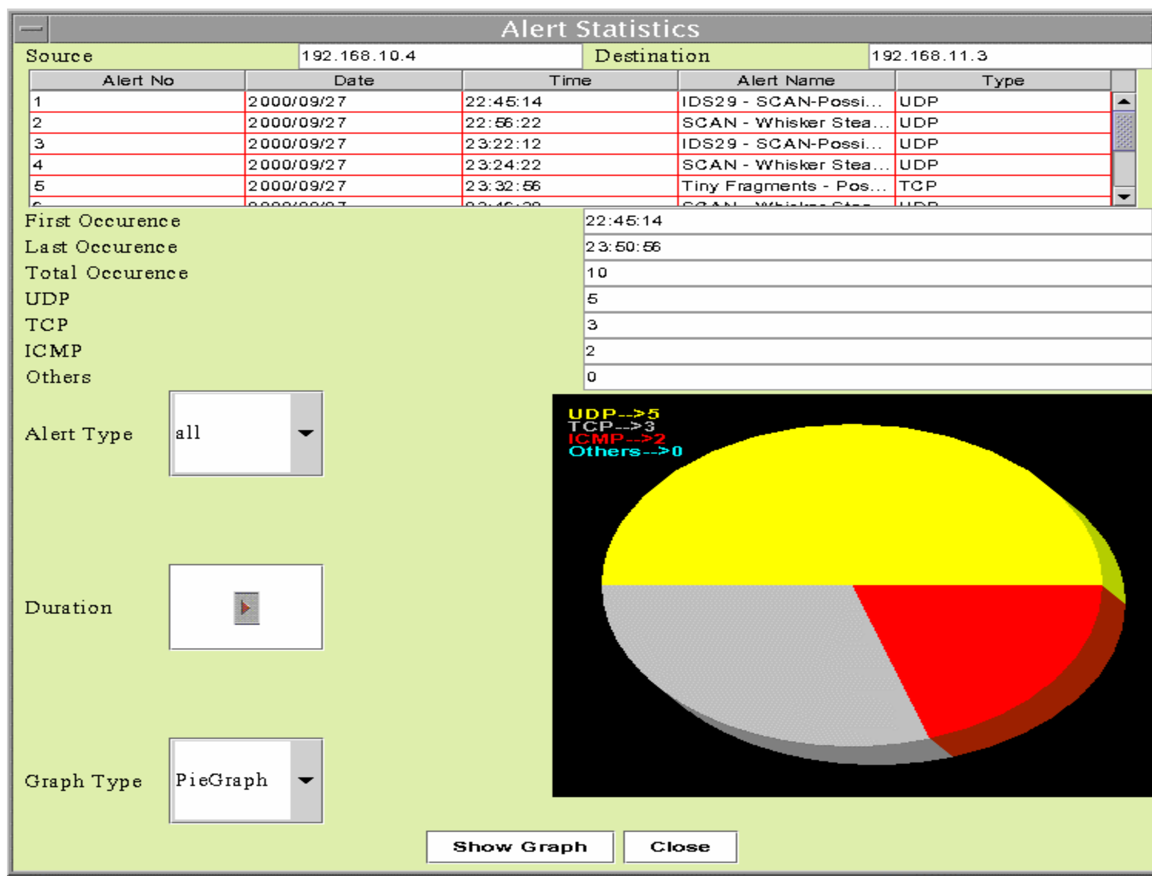
OK Cancel

“Yearly”を選択した場合には以下のようなインターフェースが表示され、この中から選ぶことができる。



“Weekly”を選択した場合には以下のようなインターフェースが表示され、この中から選ぶことができる。

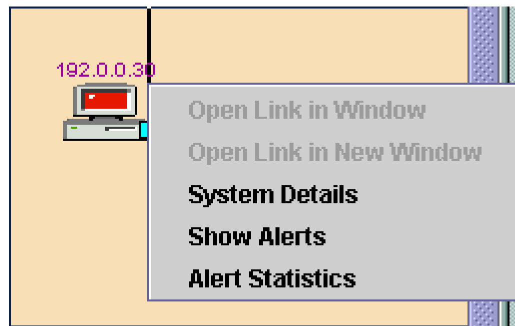




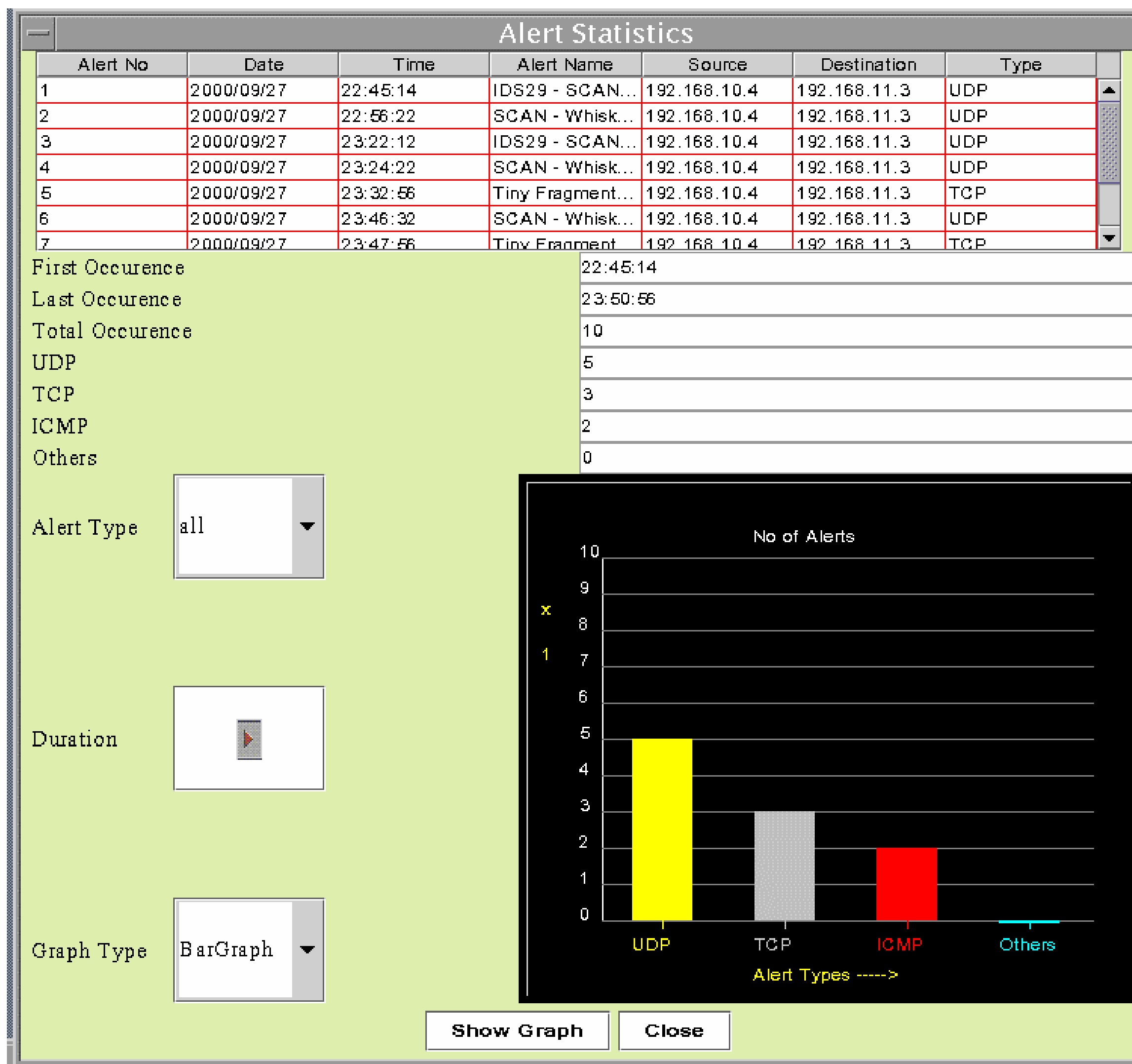
Graph Type コンボボックスでは、Bar、Pie Line などグラフの種類を選択することができる。

“Show Graph”をクリックすると、設定に基づいて(based on these selection)適切なグラフが表示される。

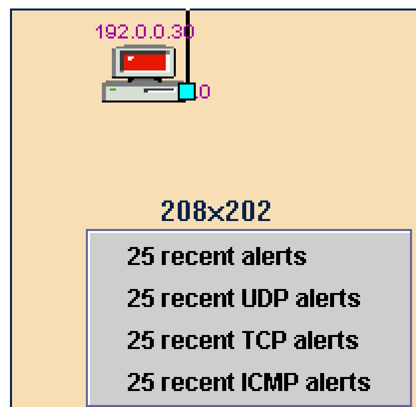
地図上の PC の上で右クリックすると、以下のようにポップアップメニューが表示される。



“Alert Statistics”を選択すると、警告に関する統計情報が表示される。



地図上で右クリックするとポップアップメニューが表示され、プロトコル別に(based on protocol)最新の警告(latest alerts)を表示する。



ポップアップメニューから選択すると、以下のように警告の詳細が適切に表示される。

